Notice of Allowability	Application No.	Applicant(s)	
	09/541,667	ELLISON ET AL.	
	Examiner	Art Unit	
	Tongoc Tran	2134	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to *7/30/2004*.

2. ☒ The allowed claim(s) is/are *1-80*.

3. ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
   a) ☐ All b) ☐ Some* c) ☐ None of the:
      1. ☐ Certified copies of the priority documents have been received.
      2. ☐ Certified copies of the priority documents have been received in Application No. _____ .
      3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

   * Certified copies not received: _____.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.
THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

4. ☐ A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.

5. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
   (a) ☐ including changes required by the Notice of Draftsperson's Patent Drawing Review (PTO-948) attached
      1) ☐ hereto or 2) ☐ to Paper No./Mail Date _____.
   (b) ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____.

Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).

6. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. ☐ Notice of References Cited (PTO-892)
2. ☐ Notice of Draftperson's Patent Drawing Review (PTO-948)
3. ☐ Information Disclosure Statements (PTO-1449 or PTO/SB/08), Paper No./Mail Date _____
4. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material
5. ☐ Notice of Informal Patent Application (PTO-152)
6. ☐ Interview Summary (PTO-413), Paper No./Mail Date _____ .
7. ☐ Examiner's Amendment/Comment
8. ☒ Examiner's Statement of Reasons for Allowance
9. ☐ Other _____.

AT

DETAILED ACTION

1. This office action is in response to Applicant's Appeal Brief filed on 7/30/2004. Claims 1-80 are pending.

Allowable Subject Matter

2. Claims 1-80 are allowed.

The following is an examiner's statement of reasons for allowance:

The claimed invention is directed to providing interface to exchange security information between a device connected to an address space of a chipset and at least one processor in an isolated execution mode in a remote attestation. The chipset is operating in a secure environment for an isolated execution mode, the secure environment being associated with an isolated memory area accessible by at least one processor operated in one of normal execution mode and an isolated execution mode.

In the remark of the Brief on pages 12 and 13, Applicant stated that the cited prior art, Davis-004, "does not disclose, expressively or inherently, (1) a secure environment for an isolated execution mode, (2) a processor operating in one of a normal execution mode and the isolated execution mode, (3) an interface to map a device to an address space of a chipset in the secure environment, and (4) a communication storage to allow the device to exchange security information with the processor in the isolated execution mode in a remote attestation".

Applicant's argument presented in the Brief disagrees with the Examiner's position, based on broadest reasonable interpretation of the claimed language, that the following disclosure taught by Davis met the above mentioned elements:

A chipset in connection (interface) with a host processor, a manipulation processing element and a main memory and a bus (Fig. 2, col. 3, line 55-col. 4, line 2). The manipulation processing element may be implemented within the host processor (normal execution mode) comprising a processing unit (isolated execution mode or IEM), a random number generator, a memory unit and an internal bus (Fig. 3A, col. 4, lines 29-58, col. 5, lines 10-12). The processing unit operated within a secure environment (IEM) (i.e. an environment with minimal vulnerability to physical or algorithm attack) and supports cryptographic operations (security information and communication storage) such as encryption/decryption, creation of a digital signature, performance of hash function and generation of keys (col. 4, lines 29-41).

In the Brief, Applicant argues that "[f]irst, Davis-004 discloses two separate processors: a host processor and a manipulation processing element, not a processor having two modes of operations. The memory unit accessible to the manipulation processing element is not accessible to the host processor (Davis-004, col. 4, lines 59-67)" (Brief, page 12, 4th paragraph).

Applicant further argues that the Examiner fails to interpret the claimed limitation in light of the Specification. Applicant stated: "[s]econd, the manipulation processing element may perform post processing and cryptographic operations, but not operations in an isolated execution mode. As supported in the Specification, the isolated execution mode includes configuration for isolated execution, definition of an isolated area, definition of isolated instructions, generation of isolated access bus cycles, and generation of isolated mode interrupts (See Specification, page 8, lines 22-25, page 9,

lines 1-2)... Here, the meaning of the isolated execution mode must be interpreted consistently with the Specification" (Brief, page 12, last paragraph – page 13, 1st paragraph); "Claims should be interpreted consistently with the Specification, which provides content for proper construction of the claims because it explains the nature of the patentee's invention. Renishaw, 158 F.3d. 1243, 48 USPQ2d 1117 (Fed. Cir. 1998). The Renishaw court explicitly states that when 'a patent applicant has elected to be a lexicographer by providing an explicit definition in the specification for a claim term,..the definition selected by the applicant controls." (Brief, page 13, 1st paragraph and page 14, 1st paragraph); "Third, Davis-004 does not discloses communication storage to allow a device to exchange security information with the processor in the isolated execution mode in a remote attestation. Davis-004 merely discloses that for authentication, digital signature may be accompanied by a digital certificate chain (Davis-004, col. 3, lines 14-16). There is no communication storage. The manipulation processing element merely performs post-processing operations on information after the information has been digitally signed (Davis-004, col. 3, lines 38-40. There is no remote attestation" (Brief, page 13, 2nd paragraph).

Therefore, in light of Applicant remark in the Brief as underlined above. The rejection has been withdrawn.

Conclusion

3. Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably

accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance."

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Tongoc Tran whose telephone number is (571) 272-3843. The examiner can normally be reached on 8:30-5:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gregory Morse can be reached on (571) 272-3838. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Examiner: Tongoc Tran
Art Unit: 2134

September 15, 2005

GREGORY MORSE
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100